Amendments to the Drawings

Replacement Sheets have been submitted for Figures 1-4 to include the legend "Related Art," in order to overcome the drawing objection.

REMARKS

Claims 1, 2, 5-8, 11-20, 23-26, and 29-54 are pending. Claims 1, 7, 8, 12, 20, 25, 32, 39, 41, 43, 44, 47, 49, and 51 have been amended, claims 3, 4, 9, 10, 21, 22, 27, and 28 have been canceled, and new claims 53 and 54 have been added to recite additional features of the embodiments disclosed in the specification. In addition, Replacement Sheets for Figures 1-4 have been submitted to overcome the drawing objection.

I. The Rejection under 35 USC § 101

Claims 1-6, 13-19, 25-31, 32-38, and 44-46 were rejected for failing to recite statutory subject matter, on grounds that the claims define an abstract idea which does not produce a tangible result. This rejection is traversed for the following reasons.

MPEP § 2106 states that process claims which do nothing more than define mathematical algorithms or manipulate abstract ideas are not patentable, because they do not recite a practical application of those algorithms or ideas. (See Section IV.B.1).

The present claims, however, do much more than recite mere abstract ideas. They recite affirmative steps that accomplish the practical application of activating a ciphering operation for call information to be transferred between a mobile communication terminal and a network. Moreover, the result of this practical application is ciphered call information, which clearly constitutes a tangible result. (See, for example, Paragraph [25] of the specification which discusses some of the tangible advantages to be produced from ciphering call data, e.g., protection against wiretapping or access to the network from unauthorized users).

This practical application and its tangible result are achieved by exchanging the messages defined in the transmitting steps of claim 1. Transmitting these messages does not involve some type of abstract idea. They constitute a real-world exchange of information (e.g., requests, request confirmations, call ciphering activation acknowledgment, etc.) between a terminal and network.

The final step involves transmitting a "ciphering activation completion message" from the network to the terminal. The words "ciphering activation completion" before "message" clearly indicate that the last-transmitted message in claim 1 informs the terminal that a ciphering activation operation has been completed, thus constituting a practical application of a tangible result.

Under MPEP § 2106, Applicants therefore submit that claim 1 and its dependent claims define patentable subject matter sufficient to satisfy the statutory requirements of 35 USC § 101.

Claim 13 recites "ciphering call information transferred between a mobile communication terminal and a network." This is accomplished by transmitting request and authentication response messages between the terminal and network, and additionally "comparing the SRES value transmitted from the terminal with the SRES value stored in the network" and "determining whether ciphering of the call information is available, depending upon whether the two SRES values are equal." These steps do not merely define the manipulation of an abstract idea, but clearly constitute a practical application of a method which produces the tangible result of determining the availability of a network to cipher call information to be transmitted between the terminal and network.

Under MPEP § 2106, such a method defines patentable subject matter under § 101.

Claim 25 recites "transmitting a ciphering request from a mobile terminal to a network" and "receiving ciphered information from the network or transmitting ciphered information to the

network after acceptance of the ciphering request." The steps of transmitting a ciphering request and then actually receiving ciphered information clearly constitutes a tangible result. Accordingly, claim 25 and its dependent claims recite patentable subject matter under § 101.

Claim 32 recites "receiving a ciphering request from a mobile terminal" and "transmitting ciphered information to the terminal or receiving ciphered information from the terminal in response to the ciphering request." These steps clearly constitute a recitation of tangible results, e.g., transmitting or receiving ciphered information is tangible. Accordingly, claim 32 and its dependent claims recite patentable subject matter under § 101.

Claim 44 recites "receiving an input signal for terminating ciphering of call information" and "transmitting a ciphering deactivation request from a mobile terminal to a network in response to the input signal." Terminating a ciphering operation clearly constitutes a tangible result. Accordingly, claim 44 and its dependent claims recite patentable subject matter under § 101.

II. The Rejection under 103(a)

Claims 1-40 and 43-52 were rejected for being obvious in view of a combination of the Al-Tawil and Arata publications. This rejection is traversed for the following reasons.

Claim 1 has been amended to recite the specific point in time when a ciphering request is transmitted from the mobile terminal to the network: "wherein the ciphering request is transmitted at a predetermined time during transfer of data from the terminal to the network, said predetermined time based on a timing of generation of a key value for ciphering activation." (See, for example, Paragraph [91]).

The Al-Tawil publication discloses transmitting a series of messages between a terminal and a network in order to activate the ciphering of information transmitted between a terminal an a network. However, unlike claim 1, these messages are transmitted during an authentication process performed during initialization. The Al-Tawil publication does not teach or suggest the features added by amendment to claim 1.

The Arata publication discloses transmitting call information between a mobile terminal and network in privacy mode. In privacy mode, a voice signal is encoded and scrambled to protect against eavesdropping. The privacy mode is set by a user of the mobile terminal. The terminal then transmits a call signal to the network which includes an indication that the call is to be performed in privacy mode.

The Arata publication, therefore, does not teach or suggest that its mobile terminal transmits a ciphering request "at a predetermined time during transfer of data from the terminal to the network, said predetermined time based on a timing of generation of a key value for ciphering activation." Absent a teaching or suggestion of these features, it is respectfully submitted that an Al-Tawil-Arata combination cannot render claim 1 or any of its dependent claims obvious.

Incidentally, it is noted that the Arata publication discloses switch from privacy mode to another mode during a call. However, this switch is performed not at the user's request but rather by a decision made by the network. More specifically, as disclosed at column 10, line 15 - column 12, when the mobile terminal travels from a cell which supports privacy mode to a cell that does not support privacy mode, the network transmits a signal to the mobile terminal indicating the same. The mobile terminal then activates a warning to notify the user that his conversation is no longer being

protected by privacy mode.

Thus, even in this embodiment, the Arata publication does not teach or suggest the features added by amendment to claim 1, including transmitting a ciphering request at a predetermined time based on a timing of generation of a key value for ciphering activation.

Claim 2 recite that the ciphering authentication request message includes a RAND value and wherein the key value is generated by the terminal based on the RAND value. The Al-Tawil publication does not teach or suggest these features, since in this system the Authentication Center AcC (i.e., the network) generates the RAND value. The Arata publication is also deficient in this respect, i.e., Arata does not teach or suggest using a random number value for activating its privacy mode.

Claims 7, 25, 32, 39, 41, and 43 have been amended to recite features similar to those which patentably distinguish claim 1 from a combination of the Al-Tawil and Arata publications. Accordingly, it is submitted that these claims and their dependent claims are also allowable.

Claim 13 recites "determining whether a RAND value is included in the ciphering request message received by the network," and "if the RAND value is included in the ciphering request message, generating a key value (Kc) required for ciphering using the RAND value, and then transmitting a ciphering activation completion message of the call information to the terminal." These features are not taught or suggested by the cited references.

As indicated above, neither reference (Al-Tawil or Arata) teaches or suggests including a RAND value in a ciphering request message transmitted from the terminal to the network. Rather, in Al-Tawil, the RAND value is generated by the network (Authentication Center) and the privacy

mode in Arata is activated without use of a random value altogether. Accordingly, the steps of determining whether a ciphering request includes a RAND value and generating a key value (Kc) based on a result of the determination are not taught or suggested by Al-Tawil and Arata.

Claim 13 further recites that "if the RAND value is not included in the ciphering request message" as after said determining step, then generating a RAND value, computing/storing an SRES value, and transmitting a ciphering authentication request message to the terminal, depending upon whether ciphering activation should be performed or not. While Al-Tawil discloses computing a RAND value and SRES value, neither Al-Tawil nor Arata teaches or suggests performing these feature if the result of the determining step indicates that a RAND value is not included in a ciphering request transmitted from the terminal to the network.

Based on these differences, it is respectfully submitted that claim 13 and its dependent claims are allowable.

Claim 20 recites that a ciphering deactivation request is transmitted from the terminal to the network "at a time when ciphered data is being transferred between the terminal and network." These features are not taught or suggested by the Al-Tawil and Arata publications. That is, while the Arata publication discloses changing modes (e.g., privacy mode to another mode) during a call, Arata does not teach or suggest that the user of the mobile terminal makes the decision to deactivate ciphering.

Accordingly, Arata does not teach or suggest transmitting a ciphering deactivation request from the terminal to the network "at a time when ciphered data is being transferred between the terminal and network." Rather, in Arata, it is the network and not the terminal that makes the decision to turn off its privacy mode. Arata does not teach or suggest turning off this mode in

response to a request message received from the mobile terminal.

Based on these differences, it is respectfully submitted that claim 20 and its dependent claims are allowable.

Claims 44, 47, 49, and 51 recite features similar to those which patentably distinguish claim 20 from the cited references. It is therefore submitted that these claims and their dependent claims are also allowable.

III. The Rejection under 102(b)

Claims 41 and 42 were rejected for being anticipated by the Arata publication. This rejection is traversed on grounds that the Arata publication does not disclose the features added by amendment to claim 1, namely that "the receiver receives the ciphering request at a predetermined time during transfer of data between the terminal and the network, said predetermined time based on a timing of generation of a key value for ciphering activation."

IV. New Claims

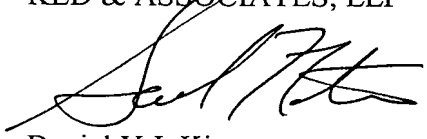
New claims 53 and 54 have been added to the application.

Claim 54 recites transmitting a ciphering deactivation request message from the terminal to the network during at a time when ciphered data is being transferred between the terminal and network. These features are not taught or suggested by the Al-Tawil and Arata publications, whether taken alone or in combination.

In view of the foregoing amendments and remarks, it is respectfully submitted that the application is in condition for allowance. Favorable consideration and timely allowance of the application are respectfully requested.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this, concurrent and future replies, including extension of time fees, to Deposit Account 16-0607 and please credit any excess fees to such deposit account.

Respectfully submitted,
KED & ASSOCIATES, LLP



Daniel Y.J. Kim
Registration No. 36,186

Samuel W. Ntiros
Registration No. 39,318

P.O. Box 221200
Chantilly, Virginia 20153-1200
(703) 766-3777
Date: June 6, 2007

Please direct all correspondence to Customer Number 34610